CLAIMS

1. A method, implemented in a computing device, the method comprising:

accessing a new security policy to be implemented by a plurality of security engines of the computing device and to be used by the plurality of security engines in place of a current security policy;

each of the plurality of security engines processing at least a portion of the new security policy to establish new rules for operation of the security engine while the security engine continues to operate according to previous rules; and

switching, after each of the plurality of security engines is ready to begin using the new security policy, each of the plurality of security engines to the new rules substantially concurrently.

2. A method as recited in claim 1, further comprising stopping the plurality of security engines from processing the at least a portion of the new security policy if one or more of the plurality of security engines indicates that the processing by the security engine failed.

3. A method as recited in claim 1, wherein for each of the plurality of security engines, the security engine is ready to begin using the new security policy after the security engine has processed the at least a portion of the new security process and can nearly ensure that it can begin using the new rules as soon as it receives an indication to switch to the new security policy.

4. A method as recited in claim 1, wherein the switching comprises calling, for each of the plurality of security engines, a function exposed by the security engine.

5. A method as recited in claim 1, wherein the switching comprises writing a value to a shared data structure.

6. A method as recited in claim 1, wherein the switching comprises firing an event across all of the security engines at once.

7. A method as recited in claim 1, wherein the plurality of security engines includes an antivirus engine.

8. A method as recited in claim 1, wherein the plurality of security engines includes a firewall engine.

9. A method as recited in claim 1, wherein the plurality of security engines includes an intrusion detection engine.

10. A method as recited in claim 1, wherein the plurality of security engines includes a vulnerability analysis engine.

11. A method as recited in claim 1, wherein the plurality of security engines includes a behavioral blocking engine.

12. A method as recited in claim 1, wherein each of the plurality of security engines is part of a same application process.

13. A method as recited in claim 1, wherein the plurality of security engines includes one or more of: an antivirus engine, a firewall engine, an intrusion detection engine, a vulnerability analysis engine, and a behavioral blocking engine.

14. A method as recited in claim 13, wherein the switching comprises one or more of:

calling, for each of the plurality of security engines, a function exposed by the security engine;

writing a value to a shared data structure; and

firing an event across all of the security engines at once.

15. One or more computer readable media having one or more instructions that, when executed by one or more processors of a device, cause the one or more processors to:

obtain a new security policy for a plurality of security engines of the device;

notify each of the plurality of security engines of one or more rules from the new security policy; and

wait until each of the plurality of security engines has indicated that it is ready to begin using the new security policy; and

after receipt of an indication that each of the plurality of security engines is ready to begin using the new security policy, instruct each of the plurality of security engines to begin using the new security policy.

16. One or more computer readable media as recited in claim 15, wherein to instruct each of the plurality of security engines to begin using the new security policy is to send a switch indication to each of the plurality of security engines substantially concurrently.

17. One or more computer readable media as recited in claim 16, wherein to send the switch indication is to call, for each of the plurality of security engines, a function exposed by the security engine.

18. One or more computer readable media as recited in claim 16, wherein to send the switch indication is to write a value to a shared data structure.

19. One or more computer readable media as recited in claim 16, wherein to send the switch indication is to fire an event across all of the security engines at once.

20. One or more computer readable media as recited in claim 15, wherein the plurality of security engines includes one or more of: an antivirus engine, a firewall engine, an intrusion detection engine, a vulnerability analysis engine, and a behavioral blocking engine.

21. One or more computer readable media as recited in claim 20, wherein to instruct each of the plurality of security engines to begin using the new security policy is to:

call, for each of the plurality of security engines, a function exposed by the security engine;

write a value to a shared data structure; and

fire an event across all of the security engines at once.

22. One or more computer readable media as recited in claim 15, wherein the one or more instructions further cause the one or more processors to issue, in response to an indication from one of the plurality of security engines that it has failed in getting ready to begin using the new security policy, an indication to each of the plurality of security engines to ignore the new security policy.

23. A method comprising:

notifying each of a plurality of security service providers in a computing device of one or more new rules;

waiting until each of the plurality of security service providers has indicated that it is ready to begin using the one or more new rules it was notified of; and

indicating, to each of the plurality of security service providers after receipt of the indications that the plurality of security service providers are ready to begin using the one or more new rules they were notified of, that the security service provider is to begin using the one or more new rules it was notified of.

24. A method as recited in claim 23, wherein each of the plurality of security service providers is notified of a different set of one or more new rules.

25. A method as recited in claim 23, wherein the indicating to each of the plurality of security service providers that the security service provider is to begin using the one or more new rules comprises calling, for each of the plurality of security service providers, a function exposed by the security service provider.

26. A method as recited in claim 23, wherein the indicating to each of the plurality of security service providers that the security service provider is to begin using the one or more new rules comprises writing a value to a shared data structure.

27. A method as recited in claim 23, wherein the indicating to each of the plurality of security service providers that the security service provider is to begin using the one or more new rules comprises firing an event across all of the security service providers at once.

28. A method as recited in claim 23, wherein the plurality of security service providers includes one or more of: an antivirus engine, a firewall engine, an intrusion detection engine, a vulnerability analysis engine, and a behavioral blocking engine.

29. A method as recited in claim 28, wherein the indicating to each of the plurality of security service providers that the security service provider is to begin using the one or more new rules comprises one or more of:

calling, for each of the plurality of security service providers, a function exposed by the security service provider;

writing a value to a shared data structure; and

firing an event across all of the security service providers at once.

30. A method as recited in claim 23, further comprising indicating, in response to an indication from one of the plurality of security service providers that it has failed in getting ready to begin using the one or more new rules it was notified of, to each of the plurality of security service providers to delete the one or more new rules it was notified of.

31. One or more computer readable media having one or more instructions that, when executed by one or more processors, causes the one or more processors to:

receive an indication of a new security policy to be used;

generate a new set of rules having associated data based on the new security policy;

continue to use a previous set of rules and associated data until an indication to begin using the new set of rules and associated data is identified; and

using, upon identifying the indication, the new set of rules and associated data.

32. One or more computer readable media as recited in claim 31, wherein the one or more instructions are part of a security engine.

33. One or more computer readable media as recited in claim 31, wherein the indication of the new security policy comprises one or more rules from which the new set of rules can be generated.

34. One or more computer readable media as recited in claim 31, wherein the indication to begin using the new set of rules and associated data is identified comprises a function exposed by the one or more instructions being invoked.

35. One or more computer readable media as recited in claim 31, wherein the indication to begin using the new set of rules and associated data is identified comprises identifying, in a shared data structure, a value indicating to begin using the new set of rules and associated data.

36. One or more computer readable media as recited in claim 31, wherein the instructions further cause the one or more processors to begin polling an event, and wherein the indication to begin using the new set of rules and associated data is identified comprises detecting that the event has been fired.

37. One or more computer readable media as recited in claim 31, wherein the one or more instructions comprises one of: an antivirus service provider, a firewall service provider, an intrusion detection service provider, a vulnerability analysis service provider, and a behavioral blocking service provider.

38. One or more computer readable media as recited in claim 37, wherein the indication to begin using the new set of rules and associated data is identified comprises one or more of:

having a function exposed by the one or more instructions invoked;

identifying, in a shared data structure, a value indicating to begin using the new set of rules and associated data; and

detecting that an event being polled has been fired.

39. One or more computer readable media as recited in claim 31, wherein the one or more instructions further cause the one or more processors to receive an indication to rollback, and in response to the indication to rollback ignore the new set of rules.

40. A method, implemented in a security engine of a computing device, the method comprising:

receiving a new set of rules to be enforced;

using a previous set of rules until an indication to begin using the new set of rules is received; and

enforcing, in response to receipt of the indication, the new set of rules.

41. A method as recited in claim 40, wherein the indication comprises having a function exposed by the security engine invoked.

42. A method as recited in claim 40, wherein the indication comprises identifying, in a shared data structure, a value indicating to begin using the new set of rules.

43. A method as recited in claim 40, wherein the indication comprises detecting that an event being polled has been fired.

44. A method as recited in claim 40, wherein the plurality of security engines includes one or more of: an antivirus engine, a firewall engine, an intrusion detection engine, a vulnerability analysis engine, and a behavioral blocking engine.

45. A method as recited in claim 44, wherein the indication comprises one or more of:

having a function exposed by the security engine invoked;

identifying, in a shared data structure, a value indicating to begin using the new set of rules and associated data; and

detecting that an event being polled has been fired.

46. A method as recited in claim 40, further comprising:

receiving an indication to ignore the new set of rules; and

in response to the indication to ignore the new set of rules, not enforcing the new set of rules but continuing to enforce the previous set of rules.

47. A system comprising:

a policy reader to obtain a new security policy to be enforced on the system;

a plurality of security service providers;

a rule set generator to generate, for each of the plurality of security service providers, a new set of rules to implement the new security policy;

a manager to send, to all of the plurality of security service providers at substantially the same time, an indication to begin using the new set of rules; and

wherein each of the plurality of security service providers continues to enforce a previous set of rules until instructed to enforce the new set of rules.

48. A system as recited in claim 47, wherein the plurality of security service providers includes one or more of: an antivirus engine, a firewall engine, an intrusion detection engine, a vulnerability analysis engine, and a behavioral blocking engine.

49. A system as recited in claim 48, wherein the manager is to send the indication by performing one or more of:

calling, for each of the plurality of security service providers, a function exposed by the security service provider;

writing a value to a shared data structure; and

firing an event across all of the security service providers at once.

50. A system comprising:

means for accessing a new security policy to be implemented by a plurality of security engines in the system, wherein the new security policy is to be used by the plurality of security engines in place of a current security policy;

means for each of the plurality of security engines to continue to operate using the current security policy until an indication is received by each of the security engines to begin using the new security policy; and

means for having each of the plurality of security engines begin using the new security policy substantially concurrently.

51. A system as recited in claim 50, wherein the means for having each of the plurality of security engines begin using the new security policy substantially concurrently comprises calling, for each of the plurality of security engines, a function exposed by the security engine.

52. A system as recited in claim 50, wherein the means for having each of the plurality of security engines begin using the new security policy substantially concurrently comprises writing a value to a shared data structure.

53. A system as recited in claim 50, wherein the means for having each of the plurality of security engines begin using the new security policy substantially concurrently comprises firing an event across all of the security engines at once.